HIPAA Compliance for the Chiropractic Practitioner What’s changed - What you need to know

Jeff Grady, HCISPP
Lead Security Solutions Advisor
Avastone Health Solutions

A division of Heartland Business Systems
Introduction

- Jeff Grady, HCISPP, Lead Security Solutions Advisor
  - Enterprise Level, as well as, Small to Medium Size Organizational Experience
  - HCISPP – what does it mean
- Goals for this presentation
  - Set the Proper Expectation: I promise you ‘will not’ become an expert in HIPAA compliance
  - My hope is to deliver some usable and practical ‘Action Items’ to improve your overall HIPAA Compliance posture - provide you with a sensible path forward – and not put you to sleep.
What has changed with HIPAA and why is it important? Some background and history:

HIPAA (Health Insurance Portability and Accountability Act) a brief history and overview of it’s evolution

• HIPAA was enacted by Congress in 1996
• Privacy Rule - The effective compliance date of the Privacy Rule was April 14, 2003.
• Security Rule - The effective date for most entities was April 20, 2005
• HIPAA Enforcement Rule – 2006
• HIPAA/HITECH enacted in 2009
• HIPAA/HITECH Final Omnibus Rule published in 1/2013 with a compliance deadline, for most of its provisions, of September 23, 2013
The Wizard of HIPAA

Why Does HIPAA Compliance Intimidate So Many?
The ‘Problem’ with HIPAA

• It was ahead of it’s time – in advance of the wide spread adoption of Electronic Health Records

• Far too much of the initial HIPAA compliance process and methodology was built for large enterprise size organizations

• Initial ‘experts’ and practitioners were naturally more comfortable with meeting compliance with the Privacy Rule and the development of ‘Policy & Procedure’ documentation - than they were with technology and data security practice

• A HIPAA compliance ‘industry’ has evolved in such a way that too often the approach to HIPAA compliance adopts an audit like mentality
Let’s Get Real About HIPAA

Once you ‘pull back the curtain’ and get to really understand HIPAA, and what’s required for compliance – it’s not so overwhelming and intimidating
Major Changes Due to the HIPAA/HITECH Rules and Regulations

• Expanded Definition of Business Associate and Application of HIPAA to Business Associates
• New Requirements for Business Associate Agreements
• New Requirements for Notice of Privacy Practices
• Expanded Patient Rights
• Increased Flexibility with PHI of Deceased Patients
• Breach Notification Threshold Standard Lowered
• Enhanced Enforcement and Civil Monetary Penalties – “Willful Neglect”
Consider the Potential Risks and Impact of Non-compliance

- Risk of OCR Audit and Fines and Potential of Breach
  - OCR just announced details on the next wave of audits
- “Willful Neglect” to support a HIPAA Finding Does Not Require Wrongful or Bad Intent
- Costs of a PHI breach
- Loss of Goodwill and Reputation as a result of breach
- Protection of sensitive data has become an expectation of both your citizens and regional government partners
- Career Impact if it happens under your ‘watch’
- Then there’s the ‘ticking time bomb’ of HIPAA compliance
A Closer Look at the Costs of a PHI Breach

- Cost of conducting a forensic investigation
- Costs of providing notice to those impacted
- Costs incurred to provide Credit and ID Fraud protection to those individuals whose information was breached
- Attorneys Fees and costs associated with the redirected staff time needed to deal with the breach
- Cost of dealing with possible OCR audit and investigation triggered by the breach
- Fines and penalties that may result from an investigation and cost of complying with any imposed remedial action plan
- Dealing with the negative publicity and loss of reputation and business
- Potential impact on career and employment status
Title: HIPAA Enforcement: Distribution of a Percentage of Civil Money Penalties or Monetary Settlements to Harmed Individuals

Abstract: This advance notice of proposed rulemaking would begin to establish a methodology under which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any civil money penalty or monetary settlement collected with respect to the offense, as required by section 13410(c)(3) of the Health Information Technology for Economic and Clinical Health Act (title XIII of the American Recovery and Reinvestment Act of 2009). The Department plans to publish an advance notice of proposed rulemaking to solicit the public's views on establishing such a methodology.

Agency: Department of Health and Human Services (HHS)  
Priority: Other Significant  
RIN Status: Previously published in the Unified Agenda  
Agenda Stage of Rulemaking: Prerule Stage  
Major: Undetermined  
Unfunded Mandates: No  
CFR Citation: 45 CFR 160  
Legal Authority: Not Yet Determined  
Legal Deadline: Action Source Description Date  
Final Statutory Deadline for issuance of regulations under HITECH 02/00/2012  

Timetable: Action Date FR Cite ANPRM 12/00/2013  
Regulatory Flexibility Analysis Required: No  
Government Levels Affected: None  
Small Entities Affected: No  
Federalism: No  
Included in the Regulatory Plan: No  
RIN Data Printed in the FR: No  
Agency Contact: Andra Wicks  
Privacy Specialist, Office of Civil Rights  
Department of Health and Human Services  
200 Independence Avenue SW., Washington, DC 20201
Why You Need To Take Action Now

- **Office for Civil Rights is moving ahead with HIPAA Audits** HHS has chosen a vendor for the next phase of the audit program and is verifying contact information for business associates and covered entities to be included under the program. OCR noted that the first audits will mostly consist of desk audits, under which it will ask entities to send in policies and procedures for review, though there may be some in-person audits as well AND, NOW WE KNOW, A WISCONSIN COUNTY HAS RECEIVED ONE OF THE OFFICIAL PRE-SCREENING COMPLIANCE AUDIT EMAILS FROM HHS/OCR

- **Finalization of rules and regulations to allow sharing of HIPAA fines with individuals harmed expected within the very near future** a/k/a ‘the ticking time bomb’ - this will likely increase reports to HHS/OCR

- **Having appropriate documentation in place to show ‘proof of compliance’ is becoming more the norm and the expectation and has become increasingly included as part of any standard ‘due diligence’ review** – both internally by an organization’s management team and by third party partners and business associates i.e. simply having a signature on a Business Associate (BA) Agreement, is no longer enough
OCR HIPAA Audit Entity Screening Questionnaire

This one ‘landed’ on a small independent physician practice in Janesville WI – and at least one Wisconsin County has received one as well.

Note:  Ten (10) Business Days to Produce Requested Documentation
Some Sample HIPAA Fines

- $1.7 Million to State of Alaska Department of Health and Human Services for Unencrypted USB Drive Stolen
- $1.7 Million to WellPoint for not properly authorizing access to an on-line application database
- $1.5 million fine to Massachusetts Eye and Ear Infirmary for a data compromise involving a lost laptop
- $4.8 Million dollar settlement fine imposed upon New York-Presbyterian Hospital and Columbia University Medical Center for a HIPAA breach impacting 6,800 individuals

- $215,000 monetary settlement payment paid by Skagit County, Washington, to settle potential violations of the privacy and security rules and agreed to comply with a three-year HIPAA compliance program under Department of Health and Human Services (HHS) jurisdiction
- $400,000 fine to Idaho State University for failing to maintain strong firewall configuration
- $150,000 fine to a twelve (12) doctor Massachusetts dermatology practice triggered by a lost thumb drive and failure to have conducted a security risk assessment along with a corrective action plan
- $50,000 penalty assessed to a non-profit hospice in Idaho for lost unencrypted laptop
- $150,000 penalty imposed upon a five-facility mental health organization in Alaska for its failure to patch their systems and continued to run outdated, unsupported software that eventually led to a malware data breach affecting 2,743 individuals.
Goal # 1 Avoid “Willful Neglect”

Why You Need To Avoid ‘Willful Neglect’

• OCR has no discretion, it must launch an investigation if there’s a showing of potential ‘willful neglect’ involved and must levy a mandatory minimum penalty if ‘willful neglect’ is found
• The mandatory minimum fines include an automatic escalator if not corrected within 30 days

<table>
<thead>
<tr>
<th>Tiers</th>
<th>Non-Compliance</th>
<th>Max Amount per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of Knowledge</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000- 50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect Corrected</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect Not Corrected</td>
<td>Mandatory Minimum $50,000 per violation</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Checklist to test Willful Neglect Exposure

Seven (7) Basic HIPAA Compliance Health Check Questions Every Covered Entity and Business Associate Needs to Ask Themselves

1. Have you conducted a legitimate HIPAA Risk Assessment (HRA) which has been documented and is not outdated?  YES ____ NO ____

2. Do you have written and appropriately updated HIPAA Privacy and Security policies in place?  YES ____ NO ____

3. Have you designated an individual trained to function in the role of your HIPAA Privacy and Security Officer?  YES ____ NO ____

4. Do you have an ongoing, documented Risk Management program?  YES___ NO ____

5. Does your organization have a documented HIPAA education, awareness and training program in operation?  YES ____ NO ____

6. Have you reviewed, revised and updated your Business Associate Agreements, as necessary?  YES ____ NO ____

7. Do you have a PHI (Protected Health Information) Breach occurrence and notification policy and process in place, and have you updated it to reflect changes made by the new HIPAA / HITECH rules?  YES ____ NO ____
Challenges to achieving ‘best practice’ HIPAA compliance

- Attitudes of: ‘HIPAA denial’ - ‘Complacent compliance’ – ‘Playing the odds’ or taking a “Let’s just wait and see” approach

- Reliance on ‘old advice’ from a few years back: “You don’t have to worry about HIPAA all you need to say is that you have a plan and that you’re working on it.”

- The main objective is achieving ‘regulatory compliance’ with your Policies and Procedure (a/k/a 3-Ring Binder Style Compliance) rather than achieving ‘best practice’ compliance and neglecting your Security Practices
  - Creates very real danger of taking comfort in what may be a false illusion of compliance
  - Caveat: The best and most expensive and updated policies and procedures in the world, if not matched by practice implementation, will not prevent a PHI breach
HIPAA Security AND Compliance

Compliance ≠ Security

Security ≠ Compliance
The Critical Importance of Proper Policy and Procedure Documentation

• In the event of an audit or breach investigation, the request for production of Policy and Procedure (P&P) documentation is one of the given expectations and a ‘must have’

• Avoid reliance on the ‘fill in the blank’ template approach

• It’s important to review your P&Ps on a regular basis to make sure they’ve been updated to reflect current law (Have yours been updated since 2013?)

• Note the difference between broad Policy language and Process and Procedure detailing of Policy implementation

• Do your operational practices and training follow and accurately reflect your P&P language?
Sample List of Security Rule Policy and Procedures

The Policies and Procedures shall include, but shall not be limited to the following:

• 1. Policies regarding encryption of ePHI.
• 2. Policies regarding password management.
• 3. Policies regarding security incident response.
• 4. Policies regarding mobile device controls.
• 5. Policies regarding information system review.
• 6. Policies regarding security reminders.
• 7. Policies regarding log-in monitoring.
• 8. Policies regarding a data backup plan.
• 9. Policies regarding a disaster recovery plan.
• 10. Policies regarding an emergency mode operation plan.
• 11. Policies regarding testing and revising of contingency plans.
• 12. Policies regarding applications and data criticality analysis.
• 13. Policies regarding automatic log off.
• 14. Policies regarding audit controls.
• 15. Policies regarding integrity controls.

This list came from a Corrective Action Plan (CAP) that arose from a HIPAA enforcement action against the Catholic Archdiocese of Philadelphia.
The Rise in Importance of the HIPAA Security Rule and the Security Risk Analysis (SRA)

Wake Up!! – it’s no longer a Three Ring Binder Policy and Procedure compliance world
Why You Need to Understand the Impact of the HIPAA Security Rule

• Since it evolved ‘later in the game’, it’s often overlooked and not as well understood
• Many of the ‘original’ HIPAA compliance experts and advisors were more familiar with the Privacy Rule and Policy & Procedure development and are not as familiar with the more technical nature of meeting the compliance mandates of the HIPAA Security Rule
• The Security Rule has specific ‘on-going’ mandates and requirements in order to maintain compliance
• Security Rule gaps have become the major focus for HHS/OCR HIPAA compliance actions  [#1 Being the lack of a proper Security Risk Analysis (SRA)]
MACRA Compliance Requires You To Conduct A HIPAA Risk Assessment
HIPAA Risk Assessment 101

• Let’s begin with what “Is Not’ a proper HIPAA Risk Assessment:
  – Vulnerability scan and penetration test reports
  – A statement from your IT staff or vendor that your networks and data are safe and secure
  – A statement from your EHR/EMR vendor that they are HIPAA compliant
Compliance Assessment vs. Risk Analysis (watch out for this confusion)

- A Compliance Assessment is a gap analysis that identifies gaps in the organization on HIPAA Administrative, Physical and Technical specifications.
- A Risk Analysis is more in depth and includes these critical elements in the report and work papers:
  - Threat Source List
  - Inventory Asset List
  - Risk Level of High, Medium and Low for each risk based on Likelihood and Impact scores
  - Likelihood determination for each risk
  - Impact determination for each risk

<table>
<thead>
<tr>
<th>RISK ASSESSMENT MATRIX</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Frequent A</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>I</td>
</tr>
<tr>
<td>Critical</td>
<td>II</td>
</tr>
<tr>
<td>Marginal</td>
<td>III</td>
</tr>
<tr>
<td>Negligible</td>
<td>IV</td>
</tr>
<tr>
<td>E-Extremely High</td>
<td>H-High</td>
</tr>
</tbody>
</table>
Steps to Conducting a HIPAA Risk Assessment for the Small to Medium Sized Covered Entity and Business Associate

Step One: Conduct full inventory of your ePHI and all your technology that in any way receives, handles, transmits or stores your ePHI. Identify and document both who grants access and who has access to your ePHI and technology network, tools and solutions.

Step Two: Identify and list the top threats and their relative risk to the confidentiality, integrity, and availability of your ePHI

Step Three: Describe and assess the effectiveness of your technology controls and protections currently in place to protect your ePHI from the likely top threats identified in Step Two

Step Four: Review current Policies and Procedures related to the HIPAA Privacy and Security Rule, as well as, Breach Notification

Step Five: Develop a plan to address any vulnerabilities identified and to implement any recommended remedial action items and improved technology controls

Note: Document all of the above
Fundamentals of a Risk Assessment
NIST SP 800-30

- Develop Inventory and Diagram Flow of all Sensitive Data
- Identify Which Applications and Technology either Creates, Receives, Maintains, Stores or Transmits Sensitive Data Electronically
- Identify and Document Potential Threats and Vulnerabilities
- Assess Current Security Controls and Measures
- Determine Likelihood and Potential Impact of Threat Occurrence
- Determine Level of Risk
- Develop Remediation and Mitigation Plan to Address Identified Gaps and Deficiencies
- REVIEW PERIODICALLY AND REPEAT THE ABOVE
1. The security risk analysis is optional for small providers.
False. All providers who are “covered entities” under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.

2. Simply installing a certified EHR fulfills the security risk analysis MU requirement.
False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.

3. My EHR vendor took care of everything I need to do about privacy and security.
False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.

4. I have to outsource the security risk analysis.
False. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.

5. A checklist will suffice for the risk analysis requirement.
False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.

6. There is a specific risk analysis method that I must follow.
False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guidance assists organizations in identifying and implementing the most effective and appropriate safeguards to secure e-PHI.
7. My security risk analysis only needs to look at my EHR.
False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager’s mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.

8. I only need to do a risk analysis once.
False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections. For more on reassessing your security practices, please see the Reassessing Your Security Practice in a Health IT Environment.

9. Before I attest for an EHR incentive program, I must fully mitigate all risks.
False. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process.

10. Each year, I’ll have to completely redo my security risk analysis.
False. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks. Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP’s year of participation in the program.
HIPAA Security Rule Compliance that benefit from input from your IT provider

- Help in conducting a proper HIPAA Security Risk Analysis
  - Insuring there exists a complete and accurate ePHI and Technology Inventory
  - Accurate description of current data security controls
  - Having input in the development of any remedial action plan to address existing gaps or areas of potential risk
- Participation and input in developing a sound ongoing Risk Management Program
- Assist in developing appropriate and mandatory HIPAA security policies and procedures
- Security Awareness Training for staff
- Insuring that you have in place a functional Breach Response and Notification plan
DIY or Obtain 3rd Party Assistance

Do you change your oil and fix your own car? Do you write your own business contracts and act as your own attorney? Do you believe and trust in everything you find on the internet? Do you use to Google to diagnose all your health complaints and concerns?

Caveat: It’s much easier and less costly to maintain a HIPAA compliance program that’s been developed with help from a Subject Matter Expert to set the foundation.

PRACTICE TIP: Best practice and advice would be to get help from a resource partner with real world experience and expertise with the HIPAA compliance rules – especially, for the critical first time, if you don’t have a solid privacy and security compliance foundation already in place.
Benefits of 3rd Party Assistance

• Brings forward an independent subject matter expert with a strong compliance message – so, it’s not just you saying this needs to get done

• Often easier for a 3rd Party to facilitate and coordinate communications between different business units or departments which is critical to establishing a compliance foundation and maintaining compliance

• Provides you with an independent 3rd Party with subject matter expertise to act in the role of a Project Manager to insure that forward progress with your HIPAA compliance initiative is made and that all work product is reviewed and attested to by someone with the necessary level of experience and expertise

• Can be helpful to have the insights and expertise of a 3rd Party who has seen a number of different environments and is familiar with a variety of alternative data security and compliance solutions – especially when developing your ongoing Risk Management Program and coming up with viable options to address any security gaps and areas needing better data security controls and remedial action.
What to Look for in a HIPAA Compliance Partner

• One that uses a Collaborative Customized Approach – and understands the maxim ‘One Size DOES NOT Fit All’
• Find a Partner Who Does Not Want to Be Viewed As Your Auditor but Rather As Your Trusted Advisor and Subject Matter Expert Guide
• Find a Partner Who is Willing to Educate and Promote Knowledge Transfer to Your Staff
• Offers a sensible and budget friendly ‘ongoing’ HIPAA compliance and maintenance solution
• Find a partner that also offers strong technology skill sets and solutions to address the critical (more technical) Security Rule within HIPAA and can assist with remediation efforts
Practice Tips to Move Forward

• Whenever possible secure ‘buy-in’ from the appropriate government oversight board or committee
• At a minimum alert and educate them to the issue and encourage them to take action to address HIPAA compliance
• It’s helpful to have all ‘stakeholders’ engaged and committed to any compliance initiative – reach out to other Department heads who are impacted by HIPAA
• One way to begin and to generate support is to have a 3rd Party conduct a baseline HIPAA compliance assessment and produce a report of your current compliance status

(Though if you’ve never conducted a Security Risk Analysis (SRA) – you’d probably want to have that as part of the deliverable)
Some Practical Observations

• **Document – Document – Document**
  • Remember to Review – Update – Revise (Compliance and especially, security compliance is never a “one and done”)
  • Avoid the ‘Off the Shelf’ Solution and taking the “Checklist to Compliance” approach
  • **Check into your Insurance Coverage – Cyber Insurance coverage** – Don’t be a passive consumer - Ask Questions
  • There is no such thing as ‘Certified HIPAA Compliant’ that is recognized by HHS/OCR
  • Be very careful of any software vendor (i.e. your EHR vendor) or insurance company who states that they have taken care of all your HIPAA compliance needs and will protect you from all risks
Practice Pointers cont.

• Don’t overspend on the unrealistic and illusionary goal of compliance perfection

• Be mindful of the concept – “reached the point of diminishing return”

• “Here’s the problem with HIPAA compliance – you’re compliant up until the point of a security event.”

• The key is to manage and control your degree of risk and eliminate exposure to ‘willful neglect’
The Case in Support of an Ongoing Compliance Solution

- HIPAA Security Rule has Periodic Required Mandates that Must be Met with Documented Proof of Ongoing Compliance
- No need or justification to redo from scratch your compliance foundation, once established
- Once ‘built’ the objective is to maintain and work upon areas that could use improvement which generally should be less costly
- Basic question to ask at the time of the periodic reviews is: “What’s Changed?” and address any changes
- Provides you with instant access to a subject matter expert in the event of a compliance question, breach or data security incident
Conducting Proper Due Diligence on a Business Associate
(P.S. This includes your IT support partner)

• Refer to Handout
Choosing the Right EHR/Cloud Solution Vendor

Research the Provider

1. Look into their reputation? Conduct an online ‘due diligence’ of reputation - are bloggers and user groups critical or supportive?
2. Conduct thorough Google searches to reveal problems. Start with a general search using the product or provider name and then move to ‘Advanced Search’ and use key phrases to locate potential critical commentary and reviews
3. How many years have they been in operation (as a SaaS vendor) ?
4. Will the vendor give you a list of other lawyers who use their product? (If so, call and check their experience.)
5. Talk to your professional friends and colleagues and the state/local Chiropractic association: are they familiar with the product or vender? What are their thoughts?
Some Practice Tips

• Retain an experienced IT professional, knowledgeable with ‘Cloud technology’ to assist you along the way (this could be your current MSP)

• Document your expectation of performance with the SaaS/Cloud Solution Vendor – might be wise to work into your communication somewhere the word ‘reliance’
Key Questions to Ask Your SaaS/Cloud Vendor

1. Where is my data stored?

2. How is my data isolated?
   
   The public cloud is a multitenant environment, which means your data is co-located alongside others’. Ask your CSP what data isolation practices they use to keep your data safe.

3. Who is responsible for what aspects of security?
   
   Many of the questions on this list deal with security and what policies the CSP has in place. But cloud security is a shared responsibility between the cloud provider and the customer, and your service-level agreement (SLA) should define who is responsible for what. To ensure the highest level of protection for your data and your networks, make sure you know what your CSP is responsible for, what you’re responsible for, and how all of these things work together.

4. How do you handle data center security?
   
   Your CSP should be able to provide details on the security measures taken at the physical location where the data is stored.

5. How secure is the cloud environment itself?
   
   Security is arguably the most important feature of any cloud. Ask your CSP for details on what they do for user authentication, access control, password protection, data encryption, firewalls, and antivirus. Access control is particularly important — a top threat to business security is disgruntled employees, followed by careless employees. Make sure you know exactly who has access to your data, both at your organization at the CSP.
Key Questions to Ask Your SaaS/Cloud Vendor cont.

6. **Will I be able to track user activities?**
   Tracking user activities allows you to ensure that only authorized people can access your data, and that they are performing only authorized operations. Ask your CSP how user activities are tracked and documented and how you can access the log files.

7. **Is my data encrypted in transit, at rest, and in use?**
   There are several levels of data encryption. Ensure that your CSP will keep your information safe at all times.

8. **How often do you conduct security assessments and audits?**
   The more often, the better.

9. **Have you ever had a security breach?**
   If the answer is “yes,” ask how it was handled and what additional security measures have been put in place since.

10. **How will I be notified in case of a security breach?**
    Some laws, such as HIPAA, have strict requirements for security breach notifications. Your CSP should have a policy covering what happens in the case that data becomes compromised in any way.

11. **Can I see your compliance reports or certifications?**
    Should be compliant with current industry standards (SSAE 16, SOC 2, SOC3). It should also be compliant with any regulations specific to your client's impact sectors (HIPAA, SOX, PCI DSS, etc.). Ask for proof.

12. **What is their track record for availability/downtime?**
    Ask for their availability/downtime history and what measures are in place to prevent unexpected service disruptions. Also find out what compensation they offer if downtime exceeds what is specified in the SLA.
13. **What is your data backup schedule?**
   How often are backups made and how far back in time do they go?

14. **What is your disaster recovery plan?**
   Ask your CSP for their disaster recovery plan so you know exactly how long it will take to get your business back up and running after a natural disaster.

15. **What happens if my data gets corrupted or lost?**
   Your CSP should have policies in place to avoid data corruption and loss. Also ask what compensation they will provide in the unlikely event that data loss does occur.

16. **Are your cloud services scalable to support my future needs?**
   Obviously, your goal is for your business to thrive and grow. Pick a CSP that will be able to support your needs into the future.

17. **What customer support services do you offer?**
   If you have a problem, is there someone you can call, even at 3 a.m.? Your CSP’s Help Desk should be available 24/7.

18. **Who owns my data in the cloud?**
   The answer should be that you do. In particular, ask your CSP about any policies they have related to metadata, or data about the data. For example, software-as-a-service (SaaS) providers often use customer data for research purposes, to generate industry benchmarks and statistics. If your data is being used in this way, make sure you know about it.
19. How long will it take to migrate to the cloud?

Your migration time will depend on what business functions you are moving to the cloud—SaaS could be close to instant, while IaaS (infrastructure-as-a-service) will take longer. If you know what to expect, you’ll be better able to prepare for the transition.

20. How will I access my data?

One of the greatest benefits of the cloud is the ability to access your data anytime, anywhere. Talk to your CSP about your data access needs. For example, do you want to restrict access to on-site computers or will your employees be able to use their own devices? Your CSP should be able to provide the access you require while taking steps to ensure your data remains secure.

21. What happens if I want to move to a different cloud service provider?

If, in two or three or five years, your CSP is no longer meeting your requirements, how easy will it be to move to another one? Ask about data portability (i.e., is your data in a format that will allow you to take it elsewhere if necessary?). Also inquire about the process of purging data from their system after a contract is terminated.
Estill County Chiropractic Patients Impacted by Ransomware Attack

On January 17, 2017, Irvine, KY-based Estill County Chiropractic discovered its computer system had been breached by an unauthorized individual who encrypted files with ransomware.

An external computer consultant was hired to conduct a thorough investigation of the incident to determine how the ransomware was installed and the extent of the attack.

While many ransomware infections occur as a result of an employee responding to a malicious spam email message, in this case, the attacker was discovered to have previously gained access to Estill County Chiropractic's computer system. Access to the system was first gained on January 6, 2017, although the ransomware was not installed until January 17.

Due to the nature of the attack, it is possible the attacker gained access to the protected health information of patients and stole patient data. The information potentially accessed included patients’ names, addresses, phone numbers, email addresses, dates of birth, clinical information, Social Security numbers, medical diagnoses, provider notes, claims information and health plan identification numbers. The investigation did not uncover any evidence to suggest that patients’ PHI had been accessed or stolen, although the possibility could not be ruled out.

Estill County Chiropractic is currently notifying affected patients that their PHI has potentially been compromised. Patients have been told that cybersecurity protections were already in place, although in response to the attack the chiropractic center’s systems have been replaced and additional security measures have been deployed to prevent future attacks.

The breach report submitted to the Department of Health and Human Services’ Office for Civil Rights indicates 5,335 patients have been impacted by the attack. Estill County Chiropractic is offering all affected patients 12 months of credit monitoring services free of charge through Equifax Personal Solutions to protect them against fraud and identity theft. Patients have been advised to exercise caution and to be vigilant to the possibility that their PHI may have been used for nefarious purposes.
Ransomware

• The goal of a ransomware attack is to hold a company's data hostage through the use of malware to infect a company's IT systems until the company pays to release that information. The malware encrypts the targeted data, which will prevent anyone other than the attacker from accessing the data files until the company complies with the attacker's demands.

• The U.S. Department of Justice has reported that an average of 4,000 ransomware attacks occur in the United States each day. According to the Federal Bureau of Investigation, U.S.-based ransomware victims reported more than $209 million in losses in the first three months of 2016 alone.
Protection Against Ransomware

Controls for Social Engineering and Phishing:

- Staff training and ongoing awareness program,
- email security,
- endpoint security,
- patch management,
- Group Policy,
- multi-factor authentication,
- next-gen firewall

A well tested Back-up and Disaster Recovery Plan
Incident Response

– Not a matter of If – but rather When  Best practice is to anticipate that it will happen at some point and have a Plan, a Documented Plan of Action in the Event of a Breach and that you Test that Plan
– Have an Internal Response Team identified in advance with a designated Team Lead and ‘back-up’
– Have your Third Party Partners in place prior
– Critical that your Action Plan include a Communication Control Plan and Protocols
– Know the laws and regulations that you’re subject to – both geographic jurisdictional and subject/sector area both general and client specific
– Have draft notices to impacted clients prepared in advance
Post Breach Response

- Identify – Contain – Control – Remediate
- Analyze the breach to determine what data was impacted and to what extent by either your in-house or outside data forensic expertise (be sure to be careful as to how you coordinate with and engage outside expertise)
- Contact your Insurance Carrier and outside Legal Counsel as appropriate
- Contact law enforcement, regulatory agencies and credit reporting agencies as necessary and appropriate
- Be prepared to sit down and communicate with your key clients from the beginning and throughout
- Address any gaps and vulnerabilities uncovered with proper remediation action and follow-up
The Elements of an Incident Response Plan

- **Internal personnel.** Identify the internal personnel responsible for each of the functions listed in the IRP. Identify them by position titles rather than by name because people come and go. A broad-based team is required for a firm of any size: management, IT, information security, human resources, compliance, marketing, etc. Have a conference call bridge line identified in case a breach happens at night or on a weekend, and include home/cell phone numbers and personal as well as work e-mail addresses. This list will need to be updated regularly as people join or leave the firm.

- **Data breach lawyer.** Identify the contact information for an experienced data breach lawyer—many large firms now have departments that focus on security and data breach response, and some smaller firms have a focus on the area. Don’t convince yourself that you can handle this without an attorney who is experienced in data breaches. Your data breach lawyer (if you selected a good one) will be an invaluable quarterback for your IRP team—and he or she may be able to preserve under attorney-client privilege much of the information related to the breach investigation.

- **Insurance policy.** Identify the location of your insurance policy (which darn well better cover data breaches). You need to make sure you are covered before you start, and list the insurer’s contact information because you are going to need to call your insurer as soon as you are aware of a possible breach.

- **Law enforcement.** Identify the contact information for law enforcement (perhaps your local FBI office), often the first folks called in.

- **Digital forensics consultant.** Identify the contact information for the digital forensics consultant you would want to investigate and remediate the cause of the breach. Often, a firm has been breached for seven months or more before the breach is discovered—it will take time to unravel what went on.

- **Containment and recovery.** Include in the IRP containment and recovery from a breach. A law firm that has been breached has an increased risk of a subsequent (or continuing) breach—either because the breach has not been fully contained or because the attacker has discovered vulnerabilities that it can exploit in the future.
Compromised data. Determine the data that has been compromised or potentially compromised. You’ll want to know if all data that should have been encrypted was indeed encrypted in transmission and in storage. If it was, this may lessen the notification burden. Identify any personally identifiable information (PII) that may have been compromised.

Systems logs. Identify and preserve systems logs for your information systems. If logging functions are not turned on or logs are not retained, start maintaining them before a breach.

Intrusion and data loss logs. If you have intrusion detection or data loss prevention software, logs from them should be preserved and provided to your investigators immediately. If you don’t, you may want to think about implementing such software.

Your bank. Identify the contact information for your bank in case your banking credentials have been compromised.

Public relations consultant (optional but often useful). Identify the contact information for a good public relations firm. If you are not required to make the breach public, you may not need one, but if it does go public, you may need to do some quick damage control. Your insurance coverage may provide for this, in which case the insurance company will put you in contact with the appropriate firm.

Clients and third parties. How will you handle any contact with clients and third parties, remembering that you may wish not to “reveal all” (if notice is not required) and yet need to achieve some level of transparency? Be forewarned that this is a difficult balance. You will feel like the victim of a data breach, but your clients will feel as though you have breached their trust in you. A data breach that becomes public can cause a mass exodus of clients, so work through your notification planning with great care. Be wary of speaking too soon before facts are fully vetted—it is a common mistake to try limiting the damage only to end up increasing it as the scope of the breach turns out to be far greater or different than first known.
Employees. How will you handle informing employees about the incident? How will you ensure that the law firm speaks with one voice and that employees do not spread information about the breach in person or online? How will your social media cover the breach, if at all?

Data breach notification law. If you have a data breach notification law in your state (and almost all do), put it right in the plan along with compliance guidelines. You may be required to contact your state attorney general. These laws vary widely, so be familiar with your own state law. Also, determine whether other states’ breach notice laws may apply owing to residences of employees or clients, location of remote offices, etc. Make sure that the relevant data breach regulations are referenced in the plan and attached to it.

Other legal obligations. Identify any impacted data that is covered by other legal obligations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or client contractual requirements, and comply with notice requirements.

Training on the plan. Conduct training on the plan. Make sure that everyone understands the plan and their role under it.

Testing the plan. Testing can range from a quick walk-through of hypothetical incidents to a full tabletop exercise. Include contacts with external resources to make sure that everything is up-to-date. This will help to make everyone familiar with the plan and to identify areas that should be revised.

Review of policies. Does the breach require that IT and information security controls and policies be updated or changed? Does what you learned from the breach require that the IRP itself be revised? The IRP should mandate at least an annual review even without an incident.
Cyber Liability Insurance

• Critically important but ‘Cyber Liability’ coverage is not always similarly defined or standardized between providers

• Some Practice Pointers on Cyber Liability coverage and issues to be aware of

• Secure advice and counsel from an Attorney experienced in Cyber Security and Compliance
Consumer Tips on Cyber Liability Coverage

• Special Note – Beware: Claim denial by the liability insurer because the insured healthcare office failed to follow “minimum required practices.” (hmmm.....might this mean failure to have conducted the required mandatory HIPAA Security Risk Analysis?)
Steps to HIPAA Compliance for the Small to Medium sized Practice and Organization

1. Conduct a proper HIPAA Security Risk Analysis, including:
   a. Full ePHI inventory and data flow description along with an inventory of all IT that handles, stores or transmits your ePHI
   b. Identify likely and potential risks and vulnerabilities to your ePHI
   c. Identify existing controls and protections and assesses their adequacy
   d. Document an action plan to address any compliance gaps or data security vulnerabilities and insures that you have an ongoing risk management program in place


3. Compile accurate list of all Business Associates and related BAAs and Documentation and conduct proper due diligence

4. Have in place and conduct proper user training on HIPAA compliance for both the Privacy and Security Rule – supplement with ongoing user awareness program


6. Insure that you have appropriate Cyber Liability coverage and that you fully understand both what it does and does not cover and the limitations on that coverage which exists

7. Make sure that you have adequate and complete back-ups for your stored data and that you have a business continuity – disaster recovery plan that has been reviewed and tested.

DOCUMENT – DOCUMENT – DOCUMENT All of the Above
Links to HIPAA Compliance and Data Security Resources

- SANS  [https://www.sans.org/critical-security-controls/](https://www.sans.org/critical-security-controls/)
- HHS.gov (Summary of the HIPAA Security Rule)  [http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html)
- HIPAA COW  [http://hipaacow.org/resources/](http://hipaacow.org/resources/)
Additional Resource Links

- HIPAA Security Series No. 7 - Security Standards: Implementation for the Small Provider
  [Link](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf?language=es)

  [Link](http://www.rscrpubs.com/Cover_Bentz_RSCR_9-21-16.pdf)

  [Link](https://transition.fcc.gov/cyber/cyberplanner.pdf)


- Small Business Information Security: The Fundamentals NISTIR 7621
  [Link](http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf)
Thank You !! ...and ‘good luck’

with your HIPAA compliance initiatives

Jeff Grady, HCISPP
igrady@hbs.net
(608) 807-0627
www.hbs.net
CIS Critical Security Controls - Version 6.0

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewall Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises
Cybercrime Prevention: Layered Defense

Layer 1: Critical Information
- Data categorization
- Application hardening

Layer 2: Physical Protection
- Physical environment
- Physical controls
- Communications
- Surveillance

Layer 3: Operating System Hardening
- Security configuration
- Anti-malware
- General ADDS security
- File system
- Print system
- .NET Framework security
- Internet Information Services
- System redundancy

Layer 4: Information Access
- User identification
- Security policies
- Resource access
- Role-based access control
- Access auditing/monitoring
- Digital rights management

Layer 5: External Access
- Perimeter networks
- VPN/RRAS
- SSTP
- PKI
- Identity federation
- NAP
Security controls will not stop a criminal. They are meant to slow them down so that you can respond before they can steal your sensitive information.

<table>
<thead>
<tr>
<th>Attacker Source</th>
<th>Network IPS</th>
<th>Firewall - Perimeter</th>
<th>Web Application Firewall</th>
<th>Firewall - DMZ Zone</th>
<th>Firewall - Internal Web Zone</th>
<th>Firewall - AD Zone</th>
<th>Firewall - Database Zone</th>
<th>Content Integrity Monitoring</th>
<th>Sensitive Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Attacker Source" /></td>
<td><img src="image" alt="Network IPS" /></td>
<td><img src="image" alt="Firewall - Perimeter" /></td>
<td><img src="image" alt="Web Application Firewall" /></td>
<td><img src="image" alt="Firewall - DMZ Zone" /></td>
<td><img src="image" alt="Firewall - Internal Web Zone" /></td>
<td><img src="image" alt="Firewall - AD Zone" /></td>
<td><img src="image" alt="Firewall - Database Zone" /></td>
<td><img src="image" alt="Content Integrity Monitoring" /></td>
<td><img src="image" alt="Sensitive Data" /></td>
</tr>
</tbody>
</table>

Threat Monitoring and Central Logging
A Solid Foundation Begins with a Plan: NIST CSF

a. Access Control
b. Awareness and Training
c. Audit and Accountability
d. Security Assessment & Authorization
e. Configuration Management
f. Contingency Planning
g. Identification and Authentication
h. Incident Response
i. Maintenance
j. Media Protection
k. Physical and Environmental Protection
l. Planning
m. Program Management
n. Personnel Security
o. Risk Assessment
p. System and Services Acquisition
q. System and Communications Protection
r. System and Information Integrity
Policies, Standard & Procedures to Support the Framework

- Acceptable Use
- Anti-Malware
- Awareness & Training
- Backup and Recovery
- Business Continuity
- BYOD
- Change Management
- Clear Desk
- Data Center Access
- Data Classification
- Data Destruction & Retention
- Disaster Recovery
- Encryption
- Exception Management
- Firewall
- Guest Network Access
- Identity & Access Management
- Incident Management
- Internet Communications
- Intrusion Detection / Prevention
- Laptop / Mobile Device
- Login Banners
- Network Access Control
- Password
- Patch Management
- Personnel Management
- Physical Security
- Policy Approval
- Remote Access
- Removable Media
- Security Logs
- Social Media Use
- Software Development
- Security Risk Assessment
- Threat Intelligence
- Visitor Access
- Vulnerability Management
- Wireless Networks
Defense-in-Depth Technology

- Anti-Malware (network perimeter and host-based)
- Firewall
- Network Access Controls (NAC)
- Intrusion Prevention Controls (IPS)
- Governance, Risk and Compliance (GRC)
- Identity and Access Management (IAM)
- Security Incident and Event Management (SIEM) & Threat Management
- Vulnerability Management
- Asset Management
- Data Loss Prevention (DLP)
- Encryption (both at rest and in transit)
- Mobile Device Management
- Database Activity Monitoring
- Password Management
- File Integrity Monitoring
### Security Rule – Administrative Safeguards – Policies & Procedures

#### Security Controls

<table>
<thead>
<tr>
<th>Access, Authorization and Authentication Controls</th>
<th>Encryption and Digital Signature Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Malware Practices</td>
<td>Incident Handling Practices</td>
</tr>
<tr>
<td>Application Development Practices</td>
<td>Logging and Auditing Practices</td>
</tr>
<tr>
<td>Asset Classification and Sensitivity Practices</td>
<td>Organizational Security Policy</td>
</tr>
<tr>
<td>Asset Management Practices</td>
<td>Password Protection Practices</td>
</tr>
<tr>
<td>Acquisition of New Company Practices</td>
<td>Patch Management Practices</td>
</tr>
<tr>
<td>Change Management Practices</td>
<td>Personnel Security Controls</td>
</tr>
<tr>
<td>Configuration Management Practices</td>
<td>Physical and Environmental Controls</td>
</tr>
<tr>
<td>Communications and Operations Management</td>
<td>Remote Access and VPN Practices</td>
</tr>
<tr>
<td>Computer System Acceptable Use Practices</td>
<td>Risk Assessment Practices</td>
</tr>
<tr>
<td>Data Backup Practices</td>
<td>Security Awareness Practices</td>
</tr>
<tr>
<td>Data Leakage Protection Controls</td>
<td>Software Licensing Practices</td>
</tr>
<tr>
<td>Data Retention Practices</td>
<td>Vendor Management Practices</td>
</tr>
<tr>
<td>Standards (R)=Required (A)=Addressable</td>
<td>Sections</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>Security Management Process (R)</strong></td>
<td>164.308(a)(1)(i)</td>
</tr>
<tr>
<td><strong>Risk Analysis (R)</strong></td>
<td>164.308(a)(1)(ii)(A)</td>
</tr>
<tr>
<td><strong>Risk Management (R)</strong></td>
<td>164.308(a)(1)(ii)(B)</td>
</tr>
<tr>
<td><strong>Sanction Policy (R)</strong></td>
<td>164.308(a)(1)(ii)(C)</td>
</tr>
<tr>
<td><strong>Information System Activity Review (R)</strong></td>
<td>164.308(a)(1)(ii)(D)</td>
</tr>
<tr>
<td><strong>Assigned Security Responsibility (R)</strong></td>
<td>164.308(a)(2)</td>
</tr>
<tr>
<td><strong>Workforce Security (R)</strong></td>
<td>164.308(a)(3)(i)</td>
</tr>
<tr>
<td>Authorization and/or Supervision (A)</td>
<td>164.308(a)(3)(ii)(A)</td>
</tr>
<tr>
<td>Workforce Clearance Procedure (A)</td>
<td>164.308(a)(3)(ii)(B)</td>
</tr>
<tr>
<td>Termination Procedures (A)</td>
<td>164.308(a)(3)(ii)(C)</td>
</tr>
</tbody>
</table>
### Information Access Management (R)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Subpart E Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Isolating Health care Clearinghouse Function (R)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Subpart E Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Access Authorization (A)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Subpart E Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Access Establishment and Modification (A)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Subpart E Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement policies and procedures that, based upon the covered entity's or the business associates' access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security Awareness and Training (R)</strong></td>
<td>164.308(a)(5)(i)</td>
<td>Implement a security awareness and training program for all members of its workforce (including management).</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Reminders (A)</td>
<td>164.308(a)(5)(ii)(A)</td>
<td>Periodic security updates.</td>
</tr>
<tr>
<td>Protection from Malicious Software (A)</td>
<td>164.308(a)(5)(ii)(B)</td>
<td>Procedures for guarding against, detecting, and reporting malicious software.</td>
</tr>
<tr>
<td>Log-in Monitoring (A)</td>
<td>164.308(a)(5)(ii)(C)</td>
<td>Procedures for monitoring log-in attempts and reporting discrepancies.</td>
</tr>
<tr>
<td>Password Management (A)</td>
<td>164.308(a)(5)(ii)(D)</td>
<td>Procedures for creating, changing, and safeguarding passwords.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Security Incident Procedures (R)</strong></th>
<th>164.308(a)(6)(i)</th>
<th>Implement policies and procedures to address security incidents.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response and Reporting (R)</td>
<td>164.308(a)(6)(ii)</td>
<td>Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.</td>
</tr>
<tr>
<td><strong>Contingency Plan (R)</strong></td>
<td>164.308(a)(7)(i)</td>
<td>Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.</td>
</tr>
<tr>
<td>Data Backup Plan (R)</td>
<td>164.308(a)(7)(ii)(A)</td>
<td>Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.</td>
</tr>
<tr>
<td>Disaster Recovery Plan (R)</td>
<td>164.308(a)(7)(ii)(B)</td>
<td>Establish (and implement as needed) procedures to restore any loss of data.</td>
</tr>
<tr>
<td>Emergency Mode Operation Plan (R)</td>
<td>164.308(a)(7)(ii)(C)</td>
<td>Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.</td>
</tr>
<tr>
<td>Testing and Revision Procedure (A)</td>
<td>164.308(a)(7)(ii)(D)</td>
<td>Implement procedures for periodic testing and revision of contingency plans.</td>
</tr>
<tr>
<td>Applications and Data Criticality Analysis (A)</td>
<td>164.308(a)(7)(ii)(E)</td>
<td>Assess the relative criticality of specific applications and data in support of other contingency plan components.</td>
</tr>
</tbody>
</table>
### Evaluation (R)

<table>
<thead>
<tr>
<th>Code</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308(a)(8)</td>
<td>Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity’s or business associate’s security policies and procedures meet the requirements of this subpart.</td>
<td></td>
</tr>
</tbody>
</table>

### BA Contracts and Other Arrangements (R)

<table>
<thead>
<tr>
<th>Code</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308(b)(1)</td>
<td>A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.</td>
<td></td>
</tr>
<tr>
<td>164.308(b)(2)</td>
<td>A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.</td>
<td></td>
</tr>
</tbody>
</table>

### Written contract or other arrangement (R)

<table>
<thead>
<tr>
<th>Code</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308(b)(3)</td>
<td>Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).</td>
<td></td>
</tr>
</tbody>
</table>
## HIPAA Security Rule Physical Safeguard Standards

<table>
<thead>
<tr>
<th>Standards (R)=Required (A)=Addressable</th>
<th>Sections</th>
<th>Specification Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facility Access Controls</strong></td>
<td>164.310(a)(1)</td>
<td>Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.</td>
</tr>
<tr>
<td><strong>Contingency operations (A)</strong></td>
<td>164.310(a)(2)(i)</td>
<td>Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.</td>
</tr>
<tr>
<td><strong>Facility Security Plan (A)</strong></td>
<td>164.310(a)(2)(ii)</td>
<td>Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.</td>
</tr>
<tr>
<td><strong>Access Control and Validation Procedures (A)</strong></td>
<td>164.310(a)(2)(iii)</td>
<td>Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.</td>
</tr>
<tr>
<td><strong>Maintenance Records (A)</strong></td>
<td>164.310(a)(2)(iv)</td>
<td>Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).</td>
</tr>
<tr>
<td><strong>Workstation Use (R)</strong></td>
<td>164.310(b)</td>
<td>Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.</td>
</tr>
<tr>
<td><strong>Workstation Security (R)</strong></td>
<td>164.310(c)</td>
<td>Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.</td>
</tr>
<tr>
<td><strong>Device and Media Controls (R)</strong></td>
<td>164.310(d)(1)</td>
<td>Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.</td>
</tr>
<tr>
<td><strong>Disposal (R)</strong></td>
<td>164.310(d)(2)(i)</td>
<td>Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.</td>
</tr>
<tr>
<td><strong>Media Re-use (R)</strong></td>
<td>164.310(d)(2)(ii)</td>
<td>Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.</td>
</tr>
<tr>
<td><strong>Accountability (A)</strong></td>
<td>164.310(d)(2)(iii)</td>
<td>Maintain a record of the movements of hardware and electronic media and any person responsible therefore.</td>
</tr>
<tr>
<td><strong>Data Backup and Storage (A)</strong></td>
<td>164.310(d)(2)(iv)</td>
<td>Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.</td>
</tr>
</tbody>
</table>
**HIPAA Security Rule Technical Safeguard Standards**

<table>
<thead>
<tr>
<th>Standards (R)=Required (A)=Addressable</th>
<th>Sections</th>
<th>Specification Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control (R)</strong></td>
<td>164.312(a)(1)</td>
<td>Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).</td>
</tr>
<tr>
<td>Unique User Identification (R)</td>
<td>164.312(a)(2)(i)</td>
<td>Assign a unique name and/or number for identifying and tracking user identity.</td>
</tr>
<tr>
<td>Emergency Access Procedure (R)</td>
<td>164.312(a)(2)(ii)</td>
<td>Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.</td>
</tr>
<tr>
<td>Automatic Logoff (A)</td>
<td>164.312(a)(2)(iii)</td>
<td>Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.</td>
</tr>
<tr>
<td>Encryption and Decryption (A)</td>
<td>164.312(a)(2)(iv)</td>
<td>Implement a mechanism to encrypt and decrypt electronic protected health information.</td>
</tr>
<tr>
<td><strong>Audit Controls (R)</strong></td>
<td>164.312(b)</td>
<td>Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</td>
</tr>
<tr>
<td><strong>Integrity (R)</strong></td>
<td>164.312(c)(1)</td>
<td>Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.</td>
</tr>
<tr>
<td>Mechanism to Authenticate ePHI (A)</td>
<td>164.312(c)(2)</td>
<td>Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.</td>
</tr>
<tr>
<td><strong>Person or Entity Authentication (R)</strong></td>
<td>164.312(d)</td>
<td>Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.</td>
</tr>
<tr>
<td><strong>Transmission Security (R)</strong></td>
<td>164.312(e)(1)</td>
<td>Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</td>
</tr>
<tr>
<td>Integrity Controls (A)</td>
<td>164.312(e)(2)(i)</td>
<td>Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.</td>
</tr>
<tr>
<td>Encryption (A)</td>
<td>164.312(e)(2)(ii)</td>
<td>Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.</td>
</tr>
<tr>
<td>BA contracts or other arrangements. (R)</td>
<td>164.314(a)(1)</td>
<td>The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.</td>
</tr>
<tr>
<td>BA contracts. (R)</td>
<td>164.314(a)(2)(i)</td>
<td>The contract must provide that the business associate will— (A) Comply with the applicable requirements of this subpart; (B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.</td>
</tr>
<tr>
<td>Other arrangements. (R)</td>
<td>164.314(a)(2)(ii)</td>
<td>The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).</td>
</tr>
<tr>
<td>Business associate contracts with subcontractors (R)</td>
<td>164.314(a)(2)(iii)</td>
<td>The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.</td>
</tr>
<tr>
<td>Requirements for group health plans. (R)</td>
<td>164.314(b)(1)</td>
<td>Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.</td>
</tr>
<tr>
<td>Implementation specifications (R)</td>
<td>164.314(b)(2)</td>
<td>The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to— (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.</td>
</tr>
<tr>
<td><strong>Policies and procedures (R)</strong></td>
<td>164.316(a)</td>
<td>Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.</td>
</tr>
<tr>
<td><strong>Documentation (R)</strong></td>
<td>164.316(b)(1)</td>
<td>(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.</td>
</tr>
<tr>
<td><strong>Time limit (R)</strong></td>
<td>164.316(b)(2)(i)</td>
<td>Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.</td>
</tr>
<tr>
<td><strong>Availability (R)</strong></td>
<td>164.316(b)(2)(ii)</td>
<td>Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.</td>
</tr>
<tr>
<td><strong>Updates (R)</strong></td>
<td>164.316(b)(2)(iii)</td>
<td>Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.</td>
</tr>
</tbody>
</table>

**Note:** Required (R) = Must implement it. Addressable (A) = Implement if reasonable and appropriate (make all attempts possible to do this). If not reasonable and appropriate, document the reason and implement an equivalent alternative measure.